year of operation. Customized reports will be prepared on a time and materials (T&M) basis. The specific rate will depend on the specific request. Mitretek will submit rates to the NANC for such customized reports. ■

7.4 Auditing

The Mitretek NANP Administration will identify and separately record all direct costs associated with providing any Enterprise Services. These costs will be reported annually to the NANC. We will obtain an audit after the first year of operations and every two years thereafter. This audit will be obtained from the same independent auditor that prepares the corporate financial statement. This audit will include an evaluation of the validity and reasonableness of the cost recorded with respect to the Enterprise Services. ■

8.0 Billing and Collection Agency Functional Requirements

Mitretek's proposal addresses only the Part 1 - NANPA/COCA functions. As we informed the NANC in our letter of 13 November 1996, we believe that to ensure neutrality of the new NANP Administration, there should be no revenue relationships directly with the telecommunications providers. Regardless of the organization selected to serve as the new NANP Administrator, we recommend that an neutral billing and collection agent, independent of the NANP Administrator, be selected. ■

9.0 Miscellaneous

9.1 Hours of Operation

The Mitretek NANP Administration will provide the telecommunications industry with daily staffing coverage during the hours of 8:15 AM Eastern to 5:00 PM Pacific. During these hours, either the Mitretek Director or Deputy Director will be available in addition to the NANP Administration staff. The business hours at each Mitretek NANP Administration location will be 8:15 AM to 5:00 PM.

The Mitretek NANP Administration Emergency Contact person will be available 24 hours a day by beeper. This person will be capable of drawing upon designated emergency personnel for operations on other than normal business hours and days.

Additionally, Mitretek NANP Administration staff will be available via voice mail, email, and facsimile during business hours and non-business hours. ■

9.2 Telecommunications Requirements

Mitretek will apply state-of-the-art voice and data processing systems to the NANP Administration requirements. In particular, information systems technology will be used to provide universal access to timely, consistent information to the NANP administrators and planners, allowing them to perform their functions more efficiently and to respond to requests from carriers and from the public. The latest World Wide Web technology will allow everyone connected to the Internet to have the latest information on number resources, recent assignments, and future plans. Finally, advanced applications such as forecasting tools and geographic information systems-based data visualization tools will allow relief planners to evaluate alternatives with more speed and precision than ever before. The following sections describe Mitretek's approach to providing automated support to the NANP Administration, the system components and functions, the technologies to be used, and a phased implementation schedule. ■

9.2.1 Voice Telecommunications Description

NANP Administration personnel will be supported with state-of-the-art telephony systems. At the McLean NANP Administration site, a PBX will provide each person with an individual phone number and a voice mailbox. Regional sites, as they are brought on-line and transitioned, will be provided with similar state-of-the-art telecommunications capabilities. Live telephone coverage during business hours will be provided by secretarial staff for all employees. Personnel answering inquiries will have access to non-proprietary data in the databases to answer questions and access to tracking data to report on the status of resource requests. Other NANP Administration remote sites will have individual phone numbers and voice mailboxes for all personnel. All NANP Administration locations will have access to an audio conferencing capability from their main meeting rooms, allowing appropriate parties who cannot attend a meeting to participate. ■

9.2.2 Information Systems Description

In developing a concept for our NANP Administration information systems, Mitretek employed the model of a "knowledge worker"[4] accessing a range of resources through a single workstation interface. Our interface will be graphically based and will present a familiar, user-friendly look, typically replicating the forms already in common use in the industry for numbering purposes. Our NANP Administration staff, based on individual identity, will have authority to view, update, and manipulate data appropriate to their function. All data will be centrally stored in two databases, one particular to traditional NANPA functions and one particular to COCA and NPA relief planning functions. Each of these databases will be backed up nightly and will be restorable on physically diverse replicas as specified in Mitretek's operational procedures. External communications will be provided through a comprehensive Internet Web site. NANP Administration personnel working remotely can access the databases with full functionality through a security

[4] A specialist in an area of expertise who applies formal education, knowledge, and skills to meet specialized needs of team-based environments, Peter Drucker.

firewall that not only allows access only to authorized users, but also provides authentication of the staff's identity. NANP Administration staff then can be granted privileges on the database as if they were locally connected. This architecture provides maximum flexibility for the Mitretek NANP Administration to extend functions into the user community.

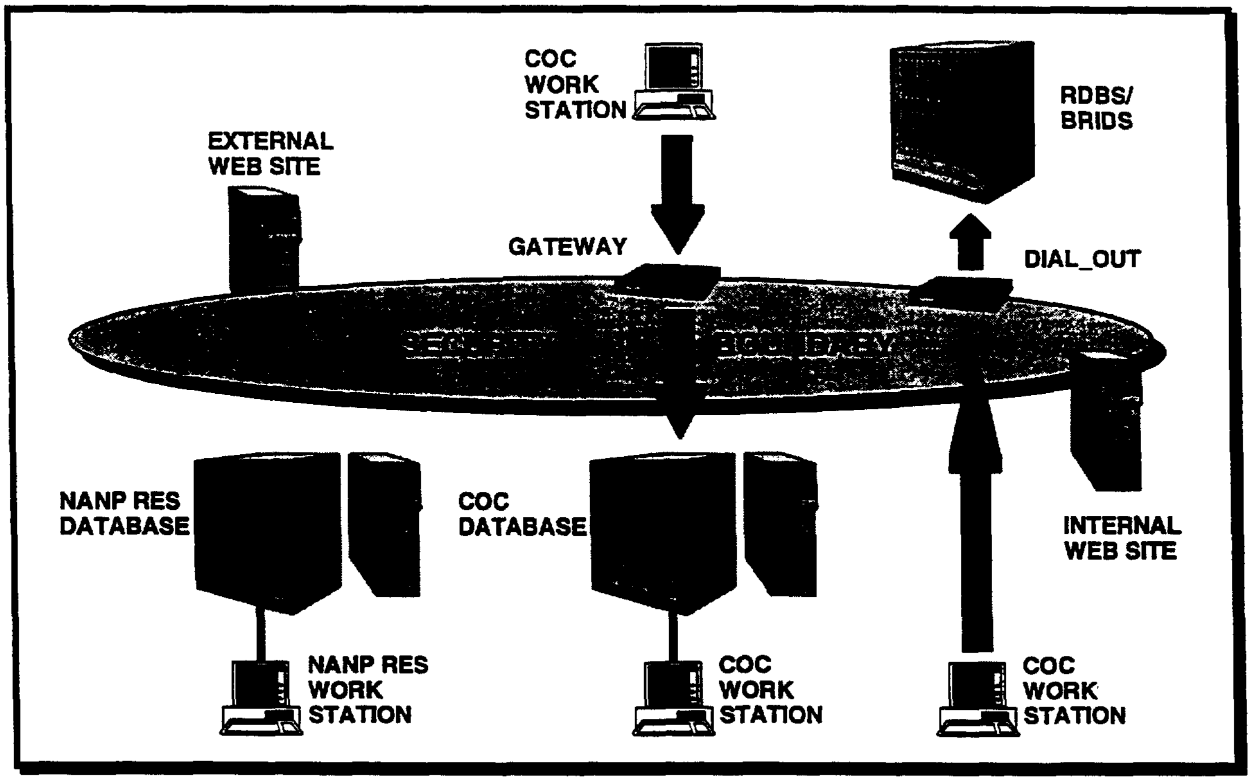

Figure 9-1. NANPA Information System Architecture

Figure 9-1 illustrates the major components of the Mitretek NANP Administration information system. NANP Administration personnel working in McLean access the databases and applications over a local area network dedicated to the NANP Administration function. A security firewall separates the local network from an external network containing the publicly visible Web Site and the gateways to the remote users. This security firewall also provides authentication for remote NANP Administration staff performing COCA functions, allowing these staff to enter codes into the COCA database. RDBS/BRIDS access is provided through a dial-out modem bank controlled by the security function.

The following sections provide more detailed information about the system components and the phased implementation plan. For each component Table 9-1 (which because of its size is included at the end of Section 9.2) enumerates:

- Component function
- Component technology
- Security mechanism
- Implementation phases for that component relative to the NANPA and COCA functions ■

9.2.2.1 Common System Components

The system components are divided into three classes:

- Those that support the NANPA functions
- Those that support the COCA functions
- Those that support both functions (common system components)

The common system components are the security boundary (including the gateway and dial-out equipment) and the internal and external Web sites. The following three sections describe these components in more detail.

9.2.2.1.1 Security Boundary

The security boundary is the only connection point between the NANP Administration internal network and the outside world. All NANP Administration electronic data, including proprietary data, is contained in databases connected to the internal network. The security boundary allows authorized users (i.e., NANP Administration personnel outside of McLean) to identify themselves absolutely and be connected to the internal network with the same privileges as if they were on the McLean network.

The security boundary computer will be a Sun Microsystems SPARC 20 running the Solaris operating system, FireWall-1 security software from Checkpoint Software Technologies, and SecurID software from Security Dynamics, Inc. Access into the security boundary computer is through a bank of dial-in modems initially operating at 28.8 kb/s, over dedicated circuits operating at 64 kb/s, or over the Internet. The boundary computer will be configured to allow users connecting over the Internet to have only access to the external Web server. Internet users will have no access to any internal NANP Administration resources. Upon connection through the modems or the dedicated circuits, the user is presented with a connection screen and must comply with the requirements of the security boundary computer to gain access to the internal network.

The initial technology that will be used for the security boundary is the SecurID technology from Security Dynamics. This method combines a smart card carried by the remote user with a password for that user. The card generates a random number each minute. The user types in his ID, a password, and the number on the card. The security boundary is also generating the same numbers as the user's card and associating them with the user's ID and password. If the user-provided password and number do not match the security machine's, then the user is rejected. This method protects against interception of the user's password and later unauthorized entry into the system. The security boundary also protects any internal systems from access by users of the external Web site.

A future implementation of the security boundary will use a secure Internet gateway in place of the dial-in modems. This gateway will employ a digital signature authentication system based on a nationally recognized certification authority. This will allow not only NANP Administration personnel to be identified, but opens the door for code requester companies to be certified for direct submission of electronic code requests to the NANP Administration. This option will be implemented when the certification infrastructure is publicly available. ■

9.2.2.1.2 Internal Web Site

The internal WWW site is located on the McLean internal network and is used by McLean-based personnel to update the information externally provided on the Web. This site is not accessible to outside staff without authentication or to the public. A user password will be required to update material on the site. At least once each day, the external Web site will be updated with the information on the internal Web site.

Initially, the data on the Web server will be manually updated by NANP Administration personnel. At the end of COC transition Phase 2, the information on the Web pages will be derived directly from non-proprietary data in the NANP resource and COC databases.

When Internet security procedures are developed to the point that absolute authentication is supported through the use of public key certificates, the database query and update functions may be performed securely through this Web site using a Web browser and forms. This functionality will be evaluated in COC transition Phase 4.

The internal Web site will be implemented on an IBM-compatible Pentium Pro server running the Windows NT/4.0 operating system and the Microsoft Internet Information Server 3 software. ■

9.2.2.1.3 External Web Site

The external Web site will be available to anyone on the Internet in a read-only mode. There will be no access to the databases through this site. The following required resource information will be posted onto this site each business day:

- NANPA Information (general information, contact names, telephone numbers, FAX numbers, e-mail addresses)
- NPA Information (assigned, reserved for NPA relief, non-available, assigned by state/region, locations served, dialing plans)
- NPA NXX Code Information (NPA-NXX assigned, carrier, effective date, NPA-NXX test numbers, unavailable NXXs, summary of assigned and available NXXs per NPA, current data reflecting relief activity)
- 900 NXX Information (assigned 900 NXX codes and carrier)
- 500 NXX Information (assigned 500 NXX codes and carrier)
- Carrier Identification Code (CIC) Information (assigned CICs and carrier)
- Vertical Service Code Information (assigned VSCs and purpose)
- 456 NXX Code Information (assigned 456 NXX codes and carrier)
- ANI II Digits Information (list of ANI II and stated purpose)
- 555-XXXX Line Number Information (assigned 555-XXXX numbers and carrier/service provider)
- N11 Service Code Information (assigned N11 codes and service description)

- 800-855 Number Information (assigned 800-855 numbers and carrier/service provider)

As new number resources are defined, information about them will also be posted. In addition, the following factual information will be included:

- Hot links to INC Number Resource Assignment Guidelines
- NANPA Information Letters relative to NPA Code Relief
- Other NANPA information as directed by NANC or appropriate regulatory bodies
- Recent NANPA Reports (within past six months)

The external Web site will be hosted in an environment that ensures continuous operation and access to sufficient bandwidth. Site activity will be monitored to assess any congestion conditions and corrective action will be taken immediately. In order to ensure the integrity of the data contained on the external Web site, the serving computer will be connected directly to the security boundary computer. The security firewall software will be configured to route only Web browser connections from the Internet to the external Web server computer. Similarly, this firewall will allow ftp connections (which can change web pages) to originate only from the NANPA internal network. As a final precaution, the following additional steps will be taken on the external Web server:

- The server will offer no services which are not absolutely required for its operation
- The Web pages will be served from a restricted set of directories

- User identification and authentication will be required on connections which can modify the web pages
- A suite of tests will be established to verify that all the restrictions are indeed working ■

9.2.2.2 NANPA Functions Components

The second class of information system components supports the staff performing the NANPA functions and is illustrated in Figure 9-2.

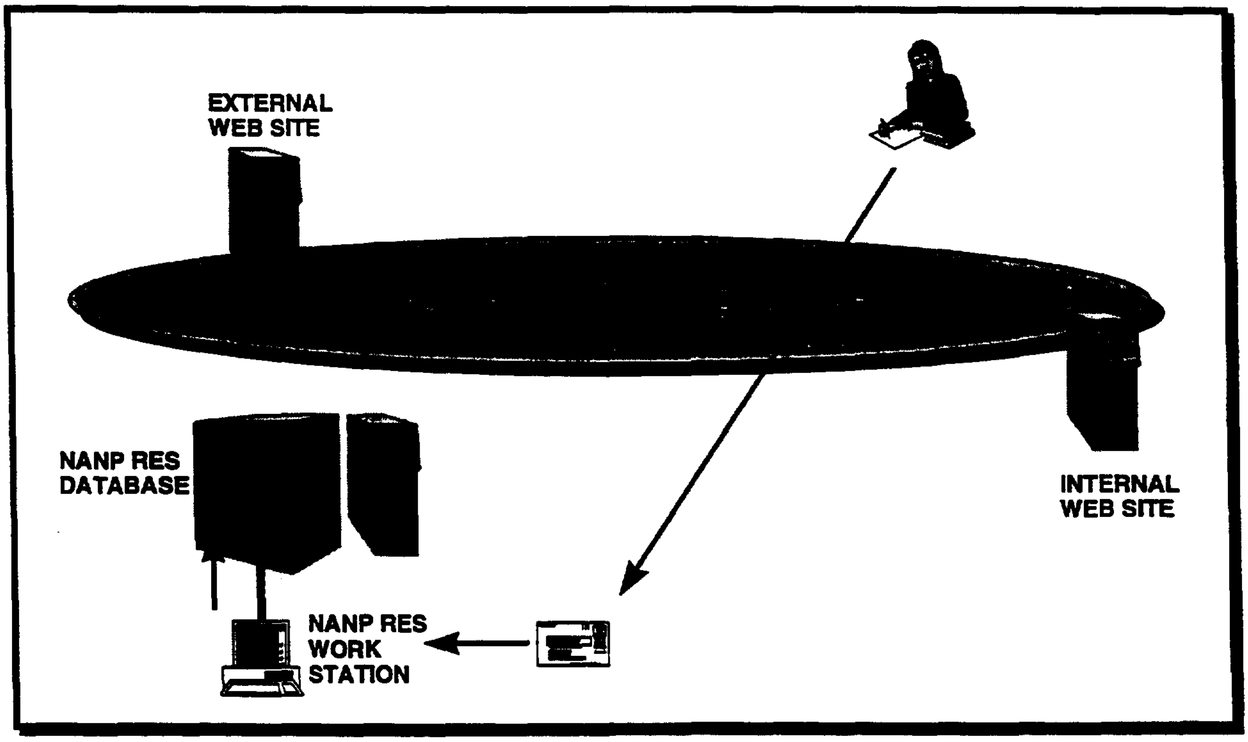

Figure 9-2. NANP Resource Components and Initial Workflow

The NANPA resource request is originated in paper form by a requester company and is physically transmitted to the NANP Administration. After verifying that the request is in accordance with current guidelines, the NANPA staff assigns a resource and enters the data into the workstation software, whose input screen is formatted identically with the resource request form. The input data is verified by the software and is entered into the NANPA resource database. The internal Web site is also updated by the administrator, which results in an update to the external Web site on the next business day.

Figure 9-3 illustrates the future workflow that will result when the secure Internet access system is implemented. The resource request is originated by a requester company by opening a secure connection to the external Web server, which has authenticated the identity of the requester. The required data is input by the requester, whose input screen is formatted identically with the resource request form. The input data is verified by the software and is entered into a staging area on the NANPA resource server, where it can be retrieved by the NANPA resource administrator. After verifying that the request is in accordance with current guidelines, the administrator assigns a resource and enters the additional data into his workstation software. The data is then verified by the software and is entered into the NANPA resource database. The internal Web site is also updated by the administrator, which results in an update to the external Web site on the next business day.

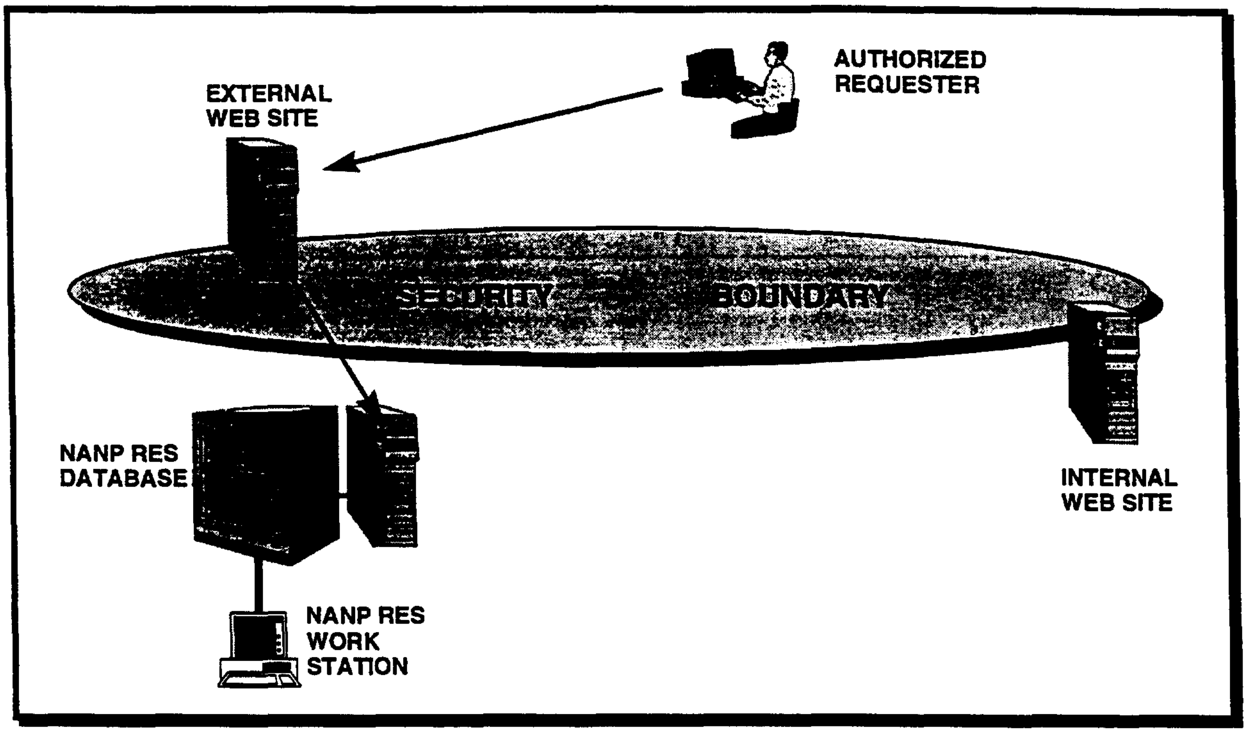

Figure 9-3. NANP Resource Components and Future Workflow

9.2.2.2.1 NANPA Resource Database

The NANPA Resource Database will house the information about the twelve number resources managed by the current NANP Administrator as described in Section 4 of this document. These resources include:

- Numbering Plan Area (NPA) Codes
- Central Office Codes (809 NPA)
- International Inbound NPA 456 NXX Codes
- PCS/N00 codes (500)

- 900 NXX Codes
- N11 Service Codes
- 800 855-XXXX Line Numbers
- 555-XXXX Line Numbers
- Carrier Identification Codes (CIC)
- Vertical Service Codes
- ANI II Digits (Information Integers)
- Non-Dialable Toll Points (NPAs 886 and 889)

This database will be hosted on an IBM-compatible Pentium Pro server running Windows NT/4.0. Microsoft SQL Server, a relational database product that is tightly coupled with Microsoft user interface and Web products, will be the database platform. The main server will reside on the NANPA internal network. The database will be backed up each night and the backup media will be stored offsite in a secure environment. In the event of an extended outage, restoral of the database at a backup site will be completed at the beginning of the next calendar day.

Each NANPA resource to be managed will reside in one or more tables within the database. Where possible, key fields in all the tables will be linked to one another, allowing views of the data to display the greatest amount of relevant information. Each table will have a list of authorized users and the permissions allowed for each user on each table. The SQL Server will communicate with client software using Microsoft's Open Database Connectivity (ODBC) product. This allows a wide range of software products access to the data, with proper authorization. The database will serve as the main source of information for reports, the external Web site, and ad hoc queries from the general public to the NANPA resource administrator. The NANPA Resource database will be operational with data populated 60 days after selection of the new NANP Administration. ■

9.2.2.2.2 NANPA Resource Workstation

The NANPA resource workstation will be the entry method into all information systems for the NANPA resource administrator. The platform will be an IBM-compatible Pentium class computer running Windows 95. Functions will be implemented in Microsoft Access, which will provide a user-friendly graphical interface and connectivity into the main SQL Server database using ODBC. The administrator will be able to query and update the NANPA resource database directly from this workstation. In most cases, the graphical user interface screen will directly correspond to an industry standard form for numbering applications. Standard reports may also be generated using data from the database. The workstation will be connected to the NANP Administration internal network and the administrator will realize his privileges in the database using a logon ID and a password.

The administrator will also be able to update NANPA resource information on the internal Web site using a password. This information will appear on the public external Web site on the next business day.

The above capabilities will be available to the Mitretek staff within the first 60 days after selection of the NANP Administration. Subsequent phases of development will add additional Web functionality to the workstation. Once true authentication is possible over the Internet, the Web browser can be used to query and update the database securely from any location. ■

9.2.2.3 COCA Function Components

The third class of information system components supports the Mitretek staff performing COCA functions. Figure 9-4 illustrates these components along with the initial workflow. In general, the application for a CO code will be sent in paper form to the regional office where it will be entered into the master COCA database by the regional COCA administrator. After verifying that the request is in accordance with current guidelines, the COCA administrator assigns a code and enters the data into his workstation software, whose input screen is formatted identically with the code request form. The input data is verified by the software and is entered into the COCA database. The internal Web site is also updated by the administrator, which results in an update to the external Web site on the next business day.

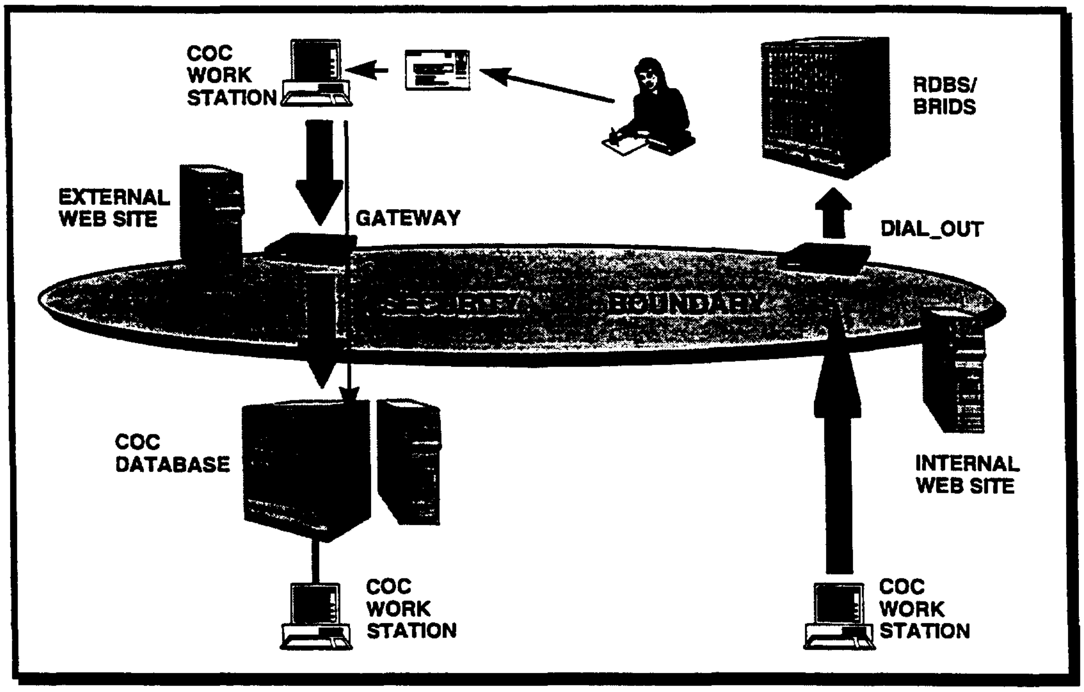

Figure 9-4. CO Code Components and Initial Workflow

Figure 9-5 illustrates the future workflow that will result when the secure Internet access system is implemented. The code request is originated by a requester company by opening a secure connection to the external Web server, which has authenticated the identity of the requester. The required data is input by the requester, whose input screen is formatted identically with the code request form. The input data is verified by the software and is entered into a staging area on the COCA server, where it can be retrieved by the CO code administrator. After verifying that the request is in accordance with current guidelines, the administrator assigns a resource and enters the additional data into his workstation software. The data is then verified by the software and is entered into the COCA

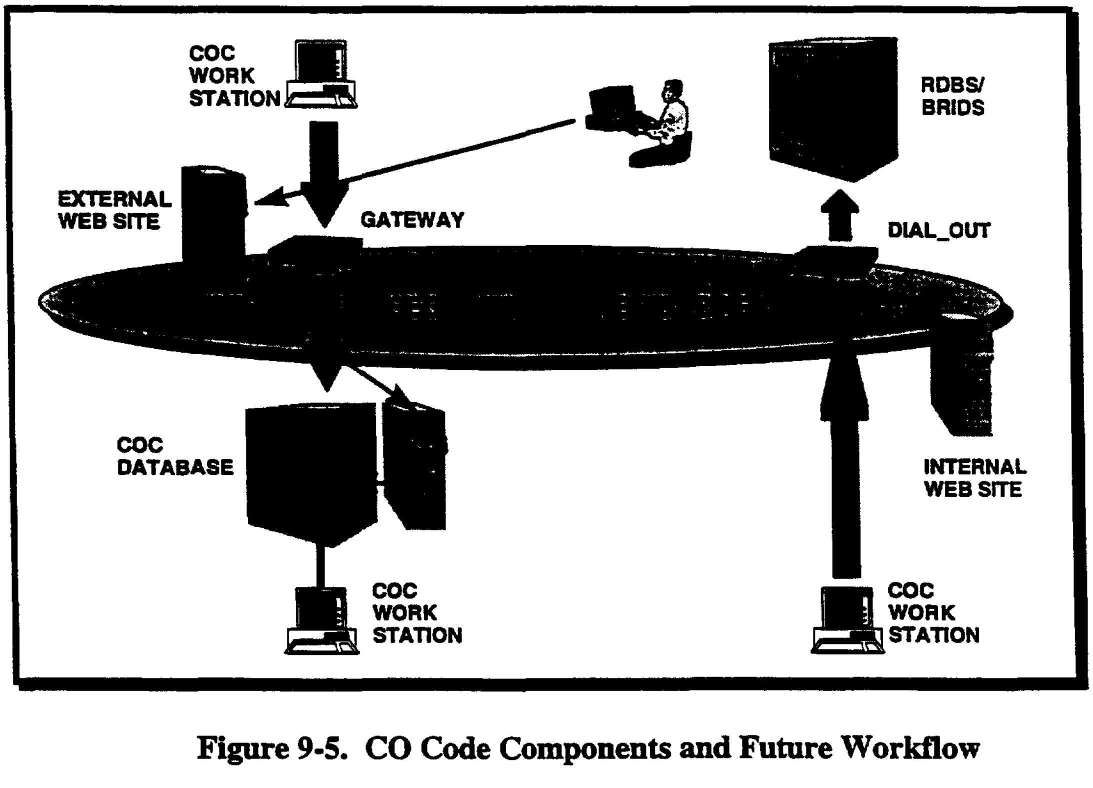

Figure 9-5. CO Code Components and Future Workflow

database. The internal Web site is also updated by the administrator, which results in an update to the external Web site on the next business day. ■

9.2.2.3.1 COCA Database

The COCA database will house all information involved with the COCA functions. This will include traditional information as contained in the LERG as well as new data elements describing the local environment needed to support relief planning (e.g., local dialing plans, NXX line utilization). Due to its size, this database will be hosted on a UNIX-based, SUN SPARCserver. This expandable, multi-processor server is an ideal platform on which to host a flexible database that must grow with the Mitretek NANP Administration needs. The latest release of an Oracle Corporation relational database will be the database platform. As with the NANPA resource server, the main server will reside on the NANP Administration internal network. A backup server will reside at a physically diverse site. Complete backups of the data in the main database will be taken each night and removed to secure, offsite storage. In the event of a protracted outage at the main site, the data will be restored at the backup site within 36 hours.

Each CO code resource to be managed will reside in one or more tables within the database. Where possible, key fields in all the tables will be linked to one another, allowing views of the data to display the greatest amount of relevant information. Each table will have a list of authorized users and the permissions allowed for each user on each table. The Oracle implemented databases will also communicate with client software using SQL*Net and the Open Database Connectivity (ODBC) product. This allows the same workstations and client software to be used for NANPA resource functions and for COCA functions. User identification and selective permissions determine the level of access in each database. The COCA database will serve as the main source of information for reports, the external Web Site, and ad hoc queries from the general public to the COC administrator. The COCA database will be operational with all its data at the end of Phase 1 of the COCA transition (see Section 5.3).

Mitretek has considerable experience in applying the configuration described above to other telecommunications management and operations applications. We have implemented complex pricing systems that collect gigabytes of traffic data and apply pricing tables to compute and optimize the overall network cost. ■

9.2.2.3.2 COCA Workstation

The COCA workstation will be similar in functionality to the NANP resource workstation except for its connection to the UNIX server and COCA database. The platform will also be an IBM-compatible Pentium class computer running Windows 95. Functions will be implemented in Microsoft Access, which will provide a user-friendly graphical interface and connectivity into the main Oracle database using SQL*Net and ODBC. The administrator will be able to query and update the COC database directly from this workstation. Standard reports may also be generated using data from the database. The workstation will be connected to the NANP Administration internal network and the staff will realize their privileges in the database using a logon ID and a password. The staff will also be able to update COCA information on the internal Web site using a password. This information will appear on the public external Web site on the next business day.

Remote COC workstations will access the NANP Administration systems over dedicated circuits operating at 64 kb/s. Dial-up modems will be available as a backup method of connectivity. The security procedures described above will be in force using either access method. The client software on the remote workstations will be the same as the clients on the internal network machines, allowing the remote sites full capability.

When full authentication procedures are available over the Internet (using public key cryptography and digital certificates), the remote NANPA sites will be able to utilize Web based client software and have full functionality using Internet access. The above capabilities will be available to the COCA administrators at the end of the transition period for appropriate COCA region. Subsequent phases of development will add additional Web functionality to the workstation. ■

9.2.2.3.3 RDBS/BRIDS Connection

Access to the Bellcore RDBS/BRIDS systems will be implemented using dial-up modems and specified security procedures for authorized users. The COCA administrators will have authorization to activate and assign carriers for new codes and will perform that function in all cases. Mitretek will also act as an Administrative Operating Company for the purposes of entering RDBS/BRIDS routing and rating data for other operating companies as specified in Section 7, Enterprise Services. The proper authorizations and registrations will be obtained to provide this function. ■

9.2.2.4 Applications

Applications are computer programs that perform specific functions and analyses on the data in order to assist the administrators in the performance of their jobs. Mitretek's technical approach is based on using information technology to improve the individual's productivity and to improve the quality of products such as NPA relief plans and exhaust forecasting by turning raw data into useful information. The following paragraphs describe applications that the Mitretek development team will implement during the first three years of its operation as NANPA.

Many of the reports required of the NANP Administration rely on large amounts of data that reside in the system databases. Software will be used wherever possible to automate the generation of the reports using the most recent data. For reports that require a mixture of text and data, the application can generate a template that contains the data and can be imported into a word processor to complete the report. Database reports can help an administrator assign codes that do not conflict with existing codes, rules, and dialing